OIPE
FEB 27 2006
PATENT & TRADEMARK OFFICE

LAW

Curtis Ikehara
99-603 Kaulainahee Place
Aiea, Hawaii 96701

February 20, 2006

Mr. Scott Au, Examiner
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

Re: Application 10/660,542

Dear Mr. Au:

Below is a response to the mailing dated 11/29/2005. Please let me know if you have any questions. You can call me at (808) 956-3581 work or (808) 488-8911. Thank you for your time.

Respectfully,

Curtis Ikehara

Detailed Response

1. Your letter states "Referring to claims 1,2,3,5,7 and 11, Kinsella discloses an input device (603) (i.e. trackball pointing device) to continuously detect biometrics for facilitating continuous authentication of the user's identification based on input from sensors attached to the device comprising (col. 3 lines 15-20): a computer mouse (603) (i.e. trackball pointing device), for providing a base with sensors that indicate different pressures applied to the base by a user (col. 18 lines 23-25) at different buttons 1,2,3;"

   The three buttons mentioned Kinsella (US# 6,914,517 - col. 18 lines 23-25) are switches as depicted schematically in Kinsella, Fig. 12. The pressures applied to the buttons are to activate a switch and do not measure different levels of pressures applied to the computer mouse. This application (10/660,542) describes pressure sensors that measures different levels of pressure as depicted in Fig. 8 of the application.

   Kinsella (US# 6,914,517) and Kharon et al. (US# 6,487,662) are both fingerprint based authentication devices. The current application (10/660,542) is based temporal detection of different pressures applied to the computer mouse. Neither Kinsella, Kharon or any of the patents sited in the letter mailed 11/29/05 refer to a the use of pressures applied to a computer mouse to continuously detect the identity of the user. In Matchett et al. (US# 5,229,764) col. 1, lines 63-68 & col. 2, lines 1-3, no mention of the pressures applied to a computer mouse is referenced. Matchett et. al's invention describes a generic analysis system, with out any specifics given to temporal biometric trait extraction from a the pressure wave produced by a use on a computer mouse. Borza et al. (US# 5,991,431) uses the fingerprint as its sole biometric identifier using an imaging system. Borza does not mention of any alternate biometric device. In Brooks (US# 6,898,299) col. 1, lines 41-47, Brooks mentions several biometric characteristics used to identify people. The pressures applied to a computer mouse are not mentioned. Brooks identified the uniqueness of the patent in Brooks claim #1, col 58, lines 38-43 as an electric field unique to the individual. This application (10/660,542) similarly uses the pressures applied to a computer mouse as unique to the individual.

2. Your letter states
   a. "an authentication computer (612) (i.e. computer verification engine), for receiving and analyzing data from the sensor electronics for registration and continuous authentication, electrically connected to said sensor electronics module (col. 19 lines 11-57);"
   b. a registration module (614) (i.e. interface controller), for initially linking the user's identity to the user's biometric characteristics, totally embedded to said authentication computer (61 2) (i.e. computer verification engine) (col. 19 lines 8-24; see Figure 14);
   c. a biometric characteristics extractor, for extracting a set of biometric characteristics from the digitized signal (col. 19 lines 49-57);
   d. a software identity database, for linking the user identity to the user's biometric characteristics in the database (col. 19 lines 49-57; see Figure 14);
   e. a continuous authentication module, for continuously verifying that the identity of a user is authorized, algorithmically connected to said registration module, and totally embedded to said authentication computer (61 2) (i.e. computer verification engine) (col. 3 lines 15-20 and col. 20 lines 1-1 0);

f. a biometrics correlation unit, for matching a new set of biometric characteristics with the biometric characteristics in the identity database (col. 19 lines 55-67); and an unauthorized user protocol, for changing the user's computer access (col. 11 lines 8-21 and col. 20 lines 15-67)."

These are analysis features common to most biometric identification devices. The component flow chart shown in Figure 5 and 6 of this application, shows those components specifically needed to process the pressures applied to a computer mouse for continuous identification. Design and algorithms may vary, but the concept is that the unique identifier, the pressures applied to a computer mouse, are processed to produce a continuous identification of the user. I do not believe Kinsella envisioned measuring the pressures applied to a computer mouse using the fingerprint sensor and circuitry or analyzing a pressure sensor signal using the Kinsella algorithms shown in figures 3, 4A, 4B, 4C or 5 of Kinsella's patent.

3. Your letter states "However, Kinsella did not explicitly disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse."

The uniqueness of this application is the biometric being identified. Kinsella used fingerprints. This application uses the different pressures applied to the computer mouse by a user. What Kinsella describes beyond the sensors is a system common to most identification systems. The difference occurs because fingerprint patterns are spatial in nature while the pressures applied to a computer mouse is temporal in nature. The system described in this application is specific for the continuous authentication of users based on the different levels of pressures applied to a computer mouse.

4. Your letter states
   a. "In the same field of endeavor of security system, Kharon et al. disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse (col. 8 lines 48-65; see Figure 4).
   b. One ordinary skill in the art understands that an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. is desirable in the security system of Kinsella because Kinsella discloses the biometl-ic data is used as an input to a computer mouse for authorizing to use a computer system (col. 4 lines 40-64) and Kharon et al. suggest a A/D converter converting the fingerprint input and verifying the data through a microcontroller 150 (col. 8 lines 48-65). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include an electrical sensor electronics module, for conditioning the analog signal so that it carl be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. in the security computer system of Kinsella with the motivation for doing so would allow the biometric data to convert into digital data in order to compare."

The analog-to-digital converter mentioned by Kharon et al. (US# 6,487,662 - col. 8

lines 48-65; see Figure 4) is a common device. Kharon is using it to convert various image intensity levels from an analog to digital form. Again, Kharon is converting fingerprint images and not pressures applied to a computer mouse. In this application, the different pressures applied to the computer mouse is converted from an analog to digital signal so that the digital computer can process it.

5. Your letter states
   a. "Referring to claim 4, Kinsella discloses input device to continuously detect biometrics in accordance with claim 1, wherein said means for receiving and analyzing data from the sensor electronics for registration and continuous authentication comprises an authentication computer (col. 12 lines 8-19; see Figure 5).
   b. Referring to claim 6, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for extracting a set of biometric characteristics from the digitized signal comprises a biometric characteristics extractor (col. 19 lines 49-57).
   c. Referring to claim 8, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for continuously verifying that the identity of a user is authorized comprises a continuous authentication module (col. 20 lines 1-10)."
   d. Referring to claim 9, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for matching a new set of biometric characteristics with the biometric characteristics in the identity database comprises a biometrics correlation unit (col. 19 lines 15-20).
   e. Referring to claim 10, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for changing the user's computer access comprises an unauthorized user protocol (col. 11 lines 15-35 and col. 19 lines 25-35).
   f. Referring to claim 12, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics as recited in claim 11, Kinsella discloses further comprising: a task computer, for providing the computer user access to a task, electrically connected to said authentication computer (col. 12 lines 8-20).
   g. Referring to claim 13, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics as claims 1 and 11, claim 13 is equivalent to that of claims 1 and 11 addressed above, incorporated herein. Therefore, claim 13 is rejected for same reasons given with respected to claims 1 and 11."

Kinsella, mentioned several biometric identifiers in col. 1, lines 56-58, but not the pressures applied to a computer mouse. It is unlikely, that Kinsella envisioned the use of the pressures applied to a computer mouse as a biometric since it had not been invented yet. Also the specialized schematics for a pressure sensor are missing from Kinsella's patent. It is unlikely, that Kinsella fingerprint biometric identification system which uses fingerprint images would work with a temporal signal like that of a pressure sensor shown in figure 5 of this application. In Brooks (US# 6,898,299) in claim #1, col 58, lines 38-43 as an electric field unique to the individual. This application (10/660,542) similarly uses the pressures

applied to a computer mouse as unique to the individual. The same reason the Brooks patent was granted, uniqueness of biometric, is precedence for this application to be granted.

scanned 11/29/06

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,542	09/12/2003	Curtis Satoru Ikehara		6416

7590 11/29/2005

Curtis Ikehara
99-603 Kaulainahee Place
Aiea, HI 96701

EXAMINER
AU, SCOTT D

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/660,542	IKEHARA ET AL.	
	Examiner	Art Unit	
	Scott Au	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The application of Ikehara et al. for an "Input device to continuously detect biometrics" filed September 12, 2003 has been examined.

Claims 1-13 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kinsella (US# 6,914,517) in view of Kharon et al. (US# 6,487,662).

Referring to claims 1,2,3,5,7 and 11, Kinsella discloses an input device (603) (i.e. trackball pointing device) to continuously detect biometrics for facilitating continuous authentication of the user's identification based on input from sensors attached to the device comprising (col. 3 lines 15-20):

a computer mouse (603) (i.e. trackball pointing device), for providing a base with sensors that indicate different pressures applied to the base by a user (col. 18 lines 23-25) at different buttons 1,2,3;

an authentication computer (612) (i.e. computer verification engine), for receiving and analyzing data from the sensor electronics for registration and continuous authentication, electrically connected to said sensor electronics module (col. 19 lines 11-57);

a registration module (614) (i.e. interface controller), for initially linking the user's identity to the user's biometric characteristics, totally embedded to said authentication computer (612) (i.e. computer verification engine) (col. 19 lines 8-24; see Figure 14);

a biometric characteristics extractor, for extracting a set of biometric characteristics from the digitized signal (col. 19 lines 49-57);

a software identity database, for linking the user identity to the user's biometric characteristics in the database (col. 19 lines 49-57; see Figure 14);

a continuous authentication module, for continuously verifying that the identity of a user is authorized, algorithmically connected to said registration module, and totally embedded to said authentication computer (612) (i.e. computer verification engine) (col. 3 lines 15-20 and col. 20 lines 1-10);

a biometrics correlation unit, for matching a new set of biometric characteristics with the biometric characteristics in the identity database (col. 19 lines 55-67); and

an unauthorized user protocol, for changing the user's computer access (col. 11 lines 8-21 and col. 20 lines 15-67).

However, Kinsella did not explicitly disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse.

In the same field of endeavor of security system, Kharon et al. disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse (col. 8 lines 48-65; see Figure 4).

One ordinary skill in the art understands that an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. is desirable in the security system of Kinsella because Kinsella discloses the biometric data is used as an input to a computer mouse for authorizing to use a computer system (col. 4 lines 40-64) and Kharon et al. suggest a A/D converter converting the fingerprint input and verifying the data through a microcontroller 150 (col. 8 lines 48-65). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. in the security computer system of Kinsella with the motivation for doing so would allow the biometric data to convert into digital data in order to compare.

Referring to claim 4, Kinsella discloses input device to continuously detect biometrics in accordance with claim 1, wherein said means for receiving and analyzing data from the sensor electronics for registration and continuous authentication comprises an authentication computer (col. 12 lines 8-19; see Figure 5).

Referring to claim 6, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for extracting a set of biometric characteristics from the digitized signal comprises a biometric characteristics extractor (col. 19 lines 49-57).

Referring to claim 8, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for continuously verifying that the identity of a user is authorized comprises a continuous authentication module (col. 20 lines 1-10).

Referring to claim 9, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for matching a new set of biometric characteristics with the biometric characteristics in the identity database comprises a biometrics correlation unit (col. 19 lines 15-20).

Referring to claim 10, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for changing the user's computer access comprises an unauthorized user protocol (col. 11 liens 15-35 and col. 19 lines 25-35).

Referring to claim 12, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics as recited in claim 11, Kinsella discloses further

comprising: a task computer, for providing the computer user access to a task, electrically connected to said authentication computer (col. 12 lines 8-20).

Referring to claim 13, Kinsella in view of Kharon et al. disclose the input device to continuously detect biometrics as claims 1 and 11, claim 13 is equivalent to that of claims 1 and 11 addressed above, incorporated herein. Therefore, claim 13 is rejected for same reasons given with respected to claims 1 and 11.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Matchett et al. (US# 5,229,764) disclose a continuous biometric authentication matrix.

Borza et al. (US# 5,991,431) disclose a mouse adapted to scan biometric data.

Brooks (US# 6,898,299) disclose a method and system for biometric recognition base on electric and /or magnetic characteristics.

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (571) 272-3063. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (571) 272-3068. The fax phone

numbers for the organization where this application or proceeding is assigned are (571)-272-1817.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

uspto.gov

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

OIPE
FEB 2 7 2006
PATENT & TRADEMARK OFFICE

Notice of References Cited	Application/Control No. 10/660,542	Applicant(s)/Patent Under Reexamination IKEHARA ET AL.	
	Examiner Scott Au	Art Unit 2635	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,914,517	07-2005	Kinsella, David J.	340/5.83
	B	US-5,229,764	07-1993	Matchett et al.	340/5.52
	C	US-6,487,662	11-2002	Kharon et al.	713/186
	D	US-5,991,431	11-1999	Borza et al.	382/127
	E	US-6,898,299	05-2005	Brooks, Juliana H. J.	382/115
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.